UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,442	01/28/2002	Robert J. Donaghey	BBNT-P02-369	5927

28120 7590 03/16/2006

FISH & NEAVE IP GROUP
ROPES & GRAY LLP
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
PIZARRO, RICARDO M	

ART UNIT	PAPER NUMBER
2662	

DATE MAILED: 03/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,442	DONAGHEY, ROBERT J.	
	Examiner	Art Unit	
	Ricardo Pizarro	2661	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,10-14,20-26,29-34,37,41,42,44 and 45* is/are rejected.

7)☒ Claim(s) *5-9,15-19,27,28,35,36,38-40 and 43* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

The abstract of the disclosure is objected to because Applicant needs to provide numbers of the US applications filed concurrently with the instant application. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-4, 10-14, 20, 25-26, 29-32, 33-34, 37 , 41-42 , 44-45 are rejected

under 35 U.S.C. 102(e) as being anticipated by US 2003/0097439 (Strayer)

Regarding claim 1, Strayer discloses a System and Methods for identifying anomalies in network data streams, comprising, including a method for modeling behavior of normal users in response to a first filtering technique (The first filtering technique being provided by the Traffic auditors 130 that sample packets of the one or more flows step 705 Fig. 7A par 0106 lines 3-6) comprising receiving a group of packets from a first user subsequent to the application of the first filtering technique (receiving packets and storing them to determine behavior step 710 in Fig. 7A, Par 0106 lines 9-11) creating at least one model reflecting the behavior of the first user based on the group of packets (Step 725 in Fig. 7A Par 0108 lines 1-3).

Regarding claim 2, Strayer discloses wherein the at least one model includes Hidden Markov Models (Par 0103 lines 5-8)

Regarding claims 3 and 26, Strayer discloses associating at least one feature with each packet in the group of packets. (Step 750 in Fig. 7a, Traceback Manager may request signatures –features – of packets, Par 0109 lines 10-12)

Regarding claim 4, wherein the at least one feature includes at least characteristics of packet headers (Par 0111 lines 20-23)

Regarding claim 10, Strayer discloses wherein the receiving includes: receiving a stream of packets from a plurality of users, identifying the packets in the stream to obtain identified first user packets, and grouping said identified first user packets (plurality of nodes and traffic auditors that identify packets in Fig. 1, Par 0023 lines 3-4, Par 0024 lines 1-3)

Regarding claim 11, Strayer discloses a system for modeling normal user behavior in a network, comprising: a memory configured to store instructions (memory 310 in Fig. 3); and a processor configured to execute the instructions (Processor 305 in Fig. 3) ; to filter packets in the network using a first filtering technique,(Traffic Auditors 130 in Fig. 3 sample and examined packets) receive a group of packets from a first user after the filtering (receiving packet and storing them to determine behavior (step 710 in Fig. 7A, Par 0106 lines 9-11) and create at least one model reflecting a behavior of the first user based on the group of packets (Step 725 in Fig. 7A Par 0108 lines 1-3).

Regarding claim 12 , Strayer discloses wherein the at least one model includes Hidden Markov Models (Par 0103 lines 5-8)

Regarding claim 13, Strayer discloses associate at least one feature with each packet in the group (Step 750 in Fig. 7A, Traceback Manager may request signatures – features – of packets, Par 0109 lines 10-12)

Regarding claim 14, Strayer discloses wherein the features include at least one characteristics of packet headers, (Par 0111 lines 20-23)

Regarding claim 20, Strayer discloses wherein when receiving the group of packets, the processor is configured to: receive a stream of packets from a plurality of users, identify the packets in the stream (plurality of nodes and traffic auditors that identify packets in Fig. 1, Par 0023 lines 3-4, Par 0024 lines 1-3)

Regarding claim 25, Strayer discloses a System and Methods for identifying anomalies in network data streams, comprising detecting an attack (Identification of anomalous or suspicious data streams in traffic flow –attack packets-, Par 0105 lines

3-4) and applying a filtering technique (The first filtering technique being provided by the Traffic auditors 130 that sample packets of the one or more flows step 705 Fig. 7A par 0106 lines 3-6) , comprising: receiving, subsequent to the filtering technique being applied, a stream of packets; partitioning the packets into groups (receiving packets and storing them in groups to determine behavior step 710 in Fig. 7A, Par 0106 lines 9-11) , each group corresponding to a plurality of packets ; classifying each group of packets as a normal group or an attack group using at least one model, each model reflecting a normal response to an application of the filtering technique (Using the developed model one or more flows can be analyzed to determine deviations from normal behavior Step 725 in Fig. 7A Par 0108 lines 6-9).and allowing the normal groups to pass on toward their destination.

Regarding claim 29, applying the filtering technique to the attack groups (traffic auditors samples packets of all the groups, par 0106 lines 3-6)

Regarding claim 30, Strayer discloses wherein the at least one model includes Hidden Markov Models (par 0103 line 5).

Regarding claim 31, wherein the at least one model relates to a filtering technique (Par 0104 15-20).

Regarding claim 32, Strayer discloses a System and Methods for identifying anomalies in network data streams, comprising: means for receiving, subsequent to a filtering technique being applied, a stream of packets(receiving packets and storing them to determine behavior step 710 in Fig. 7A, Par 0106 lines 9-11); means for partitioning the packets into groups, each group corresponding to a plurality of packets

(receiving packets and storing them in groups in a memory to determine behavior step 710 in Fig. 7A, Par 0106 lines 9-11) ; and means for classifying each group of packets as a normal group or an attack group using at least one model, each model reflecting a normal response to an application of the filtering technique (using the developed model one or more flows can be analyzed to determine deviations from normal behavior Step 725 in Fig. 7A Par 0108 lines 6-9)

Regarding claim 33, Strayer discloses a system for identifying normal traffic during a network attack, comprising a memory (memory 310 in Fig. 3) , each model reflecting a normal response to an application of a filtering technique (Using the developed model one or more flows can be analyzed to determine deviations from normal behavior therefore normal and abnormal behavior can be determined Step 725 in Fig. 7A Par 0108 lines 6-9); and a processor(Processor 305 in Fig. 3) , comprising receive a stream of packets subsequent to a first filtering technique being applied (receiving packets and storing them to determine behavior step 710 in Fig. 7A, Par 0106 lines 9-11), partitioning a stream into strands-groups- , each strand corresponding to a plurality of packets (Par 0104) , and classify each strand and at least one of a normal strand and an attack strand using at least one of the plurality of models (using the developed model one or more flows can be analyzed to determine deviations from normal behavior Step 725 in Fig. 7A Par 0108 lines 6-9)

Regarding claim 34, Strayer discloses wherein processor is further configured to allow traffic corresponding to normal strands to pass on toward their destination (Par 0109 lines 7-8)

Regarding claim 37, Strayer discloses wherein the processor is further configured to: associate at least one of a plurality of previously defined features with each packet in the stream (Step 750 in Fig. 7a, Traceback Manager may request signatures –features – of packets, Par 0109 lines 10-12)

Regarding claim 41, Strayer discloses a computer-readable medium containing instructions (memory 310 in Fig. 3) for controlling at least one processor (Processor 305 in Fig. 3) to perform a method for identifying normal traffic during a network attack, comprising: receiving, subsequent to an application of a first filtering technique, a stream of packets and grouping packets in the stream based on at least a source of the packets(receiving packets and storing them in groups and determine packets behavior step 710 in Fig. 7A, Par 0106 lines 9-11) and identifying, through the use of Hidden Markov Models each packet group as a normal group or attack group (using the developed model one or more flows can be analyzed to determine deviations from normal behavior-normal and abnormal behavior packets can be identified- Step 725 in Fig. 7A Par 0108 lines 6-9) , the HMMs representing normal responses to the application of the first filtering technique.

Regarding claim 42, Strayer discloses further comprising: associating at least one feature with each packet in the stream of packets (Step 750 in Fig. 7a, Traceback Manager may request signatures –features – of packets, Par 0109 lines 10-12)

Regarding claim 44, Strayer discloses a System and Methods for identifying anomalies in network data streams, comprising: a first device configured to create models to reflect a behavior of normal users in the network in response to an

application of at least one filtering technique (Traffic Auditor 130 in Fig. 3, Par 0028, using the developed model one or more flows can be analyzed to determine deviations from normal behavior-normal and abnormal behavior packets can be identified- Step 725 in Fig. 7A Par 0108 lines 6-9), and transmit the models; and at least one second device configured to: receive the models from the first device, use the models to identify normal traffic in the network once an attack has been detected and filtering applied (Traceback Manager 135 in Fig. 3, steps 745 and 750 in Fig. 7A that are based on developed model in step 725) , and allow identified normal traffic to pass on toward its destination .

Regarding claim 45, Strayer discloses wherein the models include Hidden Markov Models (par 0103 line 5).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 2003/0097439 (Strayer) in view of US 6,850,491 (Firoui).

Regarding claim 21, Carter discloses a computer-readable medium containing instructions (memory 310 in Fig. 3) for controlling at least one processor (Processor 305 in Fig. 3) to perform a method for identifying normal traffic during a network attack,

comprising: receiving, subsequent to an application of a first filtering technique, a stream of packets and grouping packets in the stream based on at least a source of the packets(receiving packets and storing them in groups and determine packets behavior step 710 in Fig. 7A, Par 0106 lines 9-11) and identifying, through the use of Hidden Markov Models each packet group as a normal group or attack group (using the developed model one or more flows can be analyzed to determine deviations from normal behavior-normal and abnormal behavior packets can be identified- Step 725 in Fig. 7A Par 0108 lines 6-9).

Strayer does not specifically disclose modeling behavior of users in a network in response to having at least one packet dropped.

However Firoui discloses a Modeling System in IP networks, comprising modeling flows in a computer network in response to packets being dropped (col 1 lines 61-62 and 66-67, col 2 lines 1-3)

Therefore it would have been obvious to one of ordinary skill in the art to modify Carter by providing the modeling in response to a packet being dropped as in Firoui in order to test the network behavior for proper network provisioning.

The motivation to do so is provide a method that can evaluate the performance of a network more accurately.

Regarding claim 22, Strayer discloses wherein the, at least one model includes Hidden Markov Models (par 0103 line 5) .

Regarding claim 23, Strayer discloses wherein the method further comprises: associating at least one feature with each packet from the first user, wherein the at least one feature includes characteristics of packet headers (Par 0111 lines 20-23)

Regarding claim 24 Strayer and Firou do not specifically disclose wherein the receiving includes receiving a stream of packets from a plurality of users, and grouping packets associated with the first user .

However it is well known in the art that to classify using HMMs, several HMMs may be trained on a very specific class of pattern or feature, such as grouping packets associated with a specific user. (Par 0104 lines 15-20)

Therefore it would have been obvious to one of ordinary skill in the art that grouping packets associated with a specific user, such as the first user, could have been one of the specific patterns included in the HM Markov, in order to better classify packets receive din the network.

The motivation to do so is to improve analysis of network traffic .

Allowable Subject Matter

3. Claims 5-9, 15-19, 27-28, 35-36, 38-40, 43 are rejected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claim.

Conclusion

4. **Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(571) 273-8300

(for formal communications intended for entry, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to 220 South 20th Street, Crystal Plaza Two, Lobby, Room 1B03, Arlington, Va 22202 (Customer Window).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Ricardo Pizarro** whose telephone number is (571) 272-3077. The examiner can normally be reached on Monday-Friday from 9:00 AM to 5:30 PM. .

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Hassan Kizou** can be reached on (571) 272-3088

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

2/22/2006
Ricardo Pizarro

HASSAN KIZOU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600